Cited Reference

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－134497

(43)公開日　平成11年(1999)５月21日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０６Ｔ　7/00		Ｇ０６Ｆ　15/62	４６０

審査請求　未請求　請求項の数７　ＯＬ　（全７頁）

(21)出願番号　特願平9－293820

(22)出願日　平成９年(1997)10月27日

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号

(72)発明者　小野　剛
東京都千代田区東神田２丁目８番11号　アトミック株式会社内

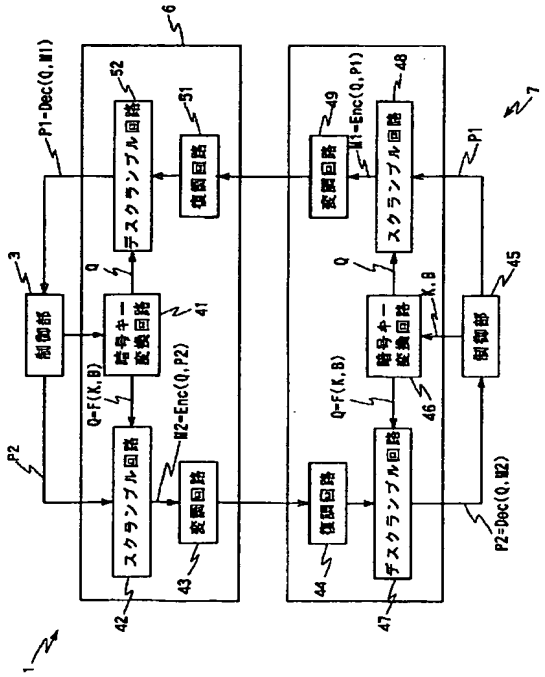
(72)発明者　塚村　善弘
東京都品川区北品川６丁目７番35号　ソニー株式会社内

(72)発明者　船橋　武
東京都品川区北品川６丁目７番35号　ソニー株式会社内

(74)代理人　弁理士　多田　繁範

(54)【発明の名称】　画像照合装置、画像照合システム、照合装置及び照合システム

(57)【要約】
【課題】本発明は、画像照合装置、画像照合システム、照合装置及び照合システムに関し、例えば画像読み取り手段と照合手段とを一体化した構成においても、十分なセキュリティーを確保できるようにする。
【解決手段】照合結果Ｐ２等を暗号化して出力するようにし、この暗号化に使用する暗号キーＱをパラメータＫ、Ｂの伝送により更新する。



【特許請求の範囲】
【請求項１】照合対象の画像を入力する画像入力手段と、
前記照合対象の画像と所定の基準画像とを照合して照合結果を出力する画像照合手段と、
前記照合結果を外部機器に出力する通信手段とを備え、
前記通信手段は、
所定の暗号キーにより前記照合結果を暗号化して出力し、
前記外部機器より伝送されるパラメータより、前記暗号キーを更新することを特徴とする画像照合装置。
【請求項２】前記通信手段は、
従前の暗号キーにより前記外部機器より入力した入力データを処理して前記パラメータを取得することを特徴とする請求項１に記載の画像照合装置。
【請求項３】前記通信手段は、
従前の暗号キーにより前記外部機器より入力した入力データを処理してデータ列を得、前記データ列に付加された位置データに基づいて、前記データ列を選択的に取り込んで前記パラメータを取得することを特徴とする請求項１に記載の画像照合装置。
【請求項４】照合対象の画像を入力する画像入力手段と、前記照合対象の画像と所定の基準画像とを照合して照合結果を出力する画像照合手段と、所定の暗号キーにより暗号化して前記照合結果を外部機器に出力する通信手段とを有する端末機器と、
前記外部機器とを有する画像照合システムであって、
前記外部機器は、
前記暗号キーの生成に必要なパラメータを、従前の暗号キーにより暗号化して前記端末機器に送出し、
前記端末機器は、
前記パラメータを取得し、該取得したパラメータにより前記従前の暗号キーを更新することを特徴とする画像照合システム。
【請求項５】前記端末機器は、
前記パラメータに、冗長なデータ、前記パラメータの位置を示す位置データ、ランダムなデータを付加して伝送することを特徴とする請求項４に記載の画像照合システム。
【請求項６】照合対象のデータを入力する入力手段と、
前記照合対象のデータと所定の基準データとを照合して照合結果を出力する照合手段と、
前記照合結果を外部機器に出力する通信手段とを備え、
前記通信手段は、
所定の暗号キーにより前記照合結果を暗号化して出力し、
前記外部機器より伝送されるパラメータより、前記暗号キーを更新することを特徴とする照合装置。
【請求項７】照合対象のデータを入力する入力手段と、
前記照合対象のデータと所定の基準データとを照合して照合結果を出力する照合手段と、所定の暗号キーにより暗号化して前記照合結果を外部機器に出力する通信手段とを有する端末機器と、
前記外部機器とを有する照合システムであって、
前記外部機器は、
前記暗号キーの生成に必要なパラメータを、従前の暗号キーにより暗号化して前記端末機器に送出し、
前記端末機器は、
前記パラメータを取得し、該取得したパラメータにより前記従前の暗号キーを更新することを特徴とする照合システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、画像照合装置、画像照合システム、照合装置及び照合システムに関し、例えばユニット化した端末機器により指紋照合する場合に適用することができる。本発明は、暗号キーにより暗号化して照合結果を伝送し、パラメータの伝送によりこの暗号キーを更新することにより、例えば画像読み取り手段と照合手段とを一体化して端末機器を構成した場合においても、十分なセキュリティーを確保できるようにする。
【０００２】
【従来の技術】従来、この種の画像照合装置でなる指紋照合装置においては、撮像手段を介して指紋の画像を読み取り、この指紋の画像より指紋の分岐、点、切れ等の特徴的な部分を抽出することにより、この特徴的な部分を基準にして指紋照合するようになされている。
【０００３】
【発明が解決しようとする課題】ところでこの種の指紋照合装置において、画像読み取り手段でなる撮像手段、指紋照合処理を実行する演算処理手段等を一体化、小型化してユニット化すれば、例えば部屋の入退出管理等に適用できると考えられる。
【０００４】ところがこのようにユニット化すると、このユニットと外部機器との間で照合結果を伝送することになり、この照合結果に対する不正な行為により、システムの安全性、信頼性が損なわれる問題がある。特に、このようなユニットと外部機器とを電話回線等の伝送路により接続する場合には、特にこの種の不正が問題となる。
【０００５】本発明は以上の点を考慮してなされたもので、例えば画像読み取り手段と照合手段とを一体化した構成においても、十分なセキュリティーを確保することができる画像照合装置、画像照合システム、照合装置及び照合システムを提案しようとするものである。
【０００６】
【課題を解決するための手段】かかる課題を解決するため本発明においては、端末機器においては、所定の暗号キーにより照合結果を暗号化して出力し、外部機器より

伝送されるパラメータよりこの暗号キーを更新する。
【０００７】また端末機器と外部機器とを有する画像照合システムにおいて、外部機器より、暗号キーの生成に必要なパラメータを、従前の暗号キーにより暗号化して端末機器に送出し、端末機器においては、このパラメータを取得し、該取得したパラメータにより従前の暗号キーを更新する。
【０００８】また照合装置及び照合システムに適用して、外部機器より伝送されるパラメータより暗号キーを更新する。
【０００９】照合結果を暗号化して伝送し、この暗号化の暗号キーを更新することにより、暗号キーの不正な取得に対応することができる。このとき外部機器より伝送されるパラメータよりこの暗号キーを更新すれば、暗号キー自体を伝送することを要しないことにより、暗号キーの不正取得を防止することができる。
【００１０】
【発明の実施の形態】以下、適宜図面を参照しながら本発明の実施の形態を詳述する。
【００１１】（１）全体構成
図２は、本発明の実施の形態に係る指紋照合装置を示すブロック図である。この指紋照合装置１は、生体検出部２、制御部３、指紋読み取り部４、画像照合部５、入出力部６が小型に一体化されたユニットにより構成される。指紋照合装置１は、このユニットが所定位置に配置されると共に、パーソナルコンピュータ等の外部機器７に接続され、例えば部屋の入退出管理等に適用される。
【００１２】この指紋照合装置１において、生体検出部２は、所定の指載置位置に指が載置されると、制御部３に通知する。
【００１３】指紋読み取り部４は、制御部３の制御によりこの指載置位置に載置された指の画像を撮像し、ビデオ信号ＳＶを出力する。
【００１４】画像照合部５は、制御部３の制御により動作モードを切り換え、このビデオ信号ＳＶを２値化して画像データを生成する。また画像照合部５は、指紋登録モードにおいて、この指紋データＤ１、又は入出力部６を介して入力される指紋データを内蔵のデータベースに登録する。これにより画像照合部５は、この指紋登録モードにおいて、指紋照合の基準となる基準画像を登録する。
【００１５】また指紋照合モードにおいて、このようにして内蔵のデータベースに登録した基準画像と、所定の指紋データによる指紋画像と照合し、照合結果を出力する。ここでこの指紋照合装置１において、指紋照合モードは、生体検出部２の検出結果をトリガにして、画像照合部５に保持した基準画像と指紋読み取り部４を介して得られる指紋画像とを照合する第１の自己照合モードと、外部機器７の指示をトリガにして画像照合部５に保持した基準画像と指紋読み取り部４より得られる指紋画像とを照合する第２の自己照合モードと、外部機器７の指示により画像照合部５に保持した基準画像と外部機器７より入力される指紋画像とを照合する第２の外部照合モードとにより構成される。
【００１６】画像照合部５は、これら３つの指紋照合モードに対応して、それぞれ指紋読み取り部４を介して得られる指紋画像、入出力部６を介して外部機器７より入力される指紋画像を照合対象に設定して、データベースに保持した基準画像との間で指紋照合の処理を実行する。
【００１７】入出力部６は、制御部３の制御により、外部機器７より入力される制御コマンドを制御部３に通知し、また外部機器より入力される画像データを画像照合部５に出力し、さらに画像照合部５による照合結果を外部機器７に出力する。
【００１８】制御部３は、この指紋照合装置１全体の動作を制御するマイクロコンピュータにより構成され、外部機器７の制御により動作モードを設定する。
【００１９】（１－１）入出力部の処理
図１は、指紋照合装置１の入出力部６と外部機器７との接続を示すブロック図である。この指紋照合装置１においては、外部機器７との間で入出力する各種データを図３に示すフォーマットによるメッセージＰ１及びＰ２に変換し、このメッセージＰ１及びＰ２を暗号化して伝送する。
【００２０】すなわち制御部３は、外部機器７に対して、ステータス、照合結果等を送出する場合に、このステータス、照合結果をメッセージ部に割り当てて所定のパケットを形成する。このとき制御部３は、このパケットに冗長なデータを割り当てて一定のデータ量に設定した後、メッセージ部の位置を示す位置データ、ランダムなデータを割り当てる。これにより制御部３は、このパケットによるメッセージＰ１を所定の暗号キーによりスクランブル処理し、いわゆるＳＡＬＴの手法により同一のメッセージ部を送出する場合でも、その都度異なるデータにより送出するようになされている。
【００２１】すなわち入出力部６において、暗号キー変換回路４１は、制御部３より出力されるオリジナルパラメータＫ、変換パラメータＢを受け、これらのパラメータＢ、Ｋより所定の演算処理を実行することにより暗号キーＱ（＝Ｆ（Ｋ，Ｂ））を生成する。なおここでＦ（Ｋ，Ｂ）は、パラメータＢ、Ｋより暗号キーＱを作成する関数である。
【００２２】スクランブル回路４２は、制御部３より出力されるメッセージＰ２をこの暗号キーＱ（＝Ｆ（Ｋ，Ｂ））によりスクランブル処理し、これにより暗号化データＭ２（＝Ｅｎｃ（Ｑ、Ｐ２））を生成する。なおここでＥｎｃ（Ｑ、Ｐ２）は、暗号キーＱによりメッセージＰ２を暗号化する関数である。
【００２３】変調回路４３は、スクランブル回路４２よ

り出力される暗号化データをシリアルデータ列に変換した後、この指紋照合装置１が外部機器と接続される伝送路に適した変調方式により、変調して出力する。

【００２４】これらの処理に対応して、外部機器７においては、復調回路４４において、伝送路を介して入力される暗号化データを復号する。また演算処理回路等により構成される制御部４５より暗号キー変換回路４６に指紋照合装置１と同一のパラメータＫ、Ｂを設定し、指紋照合装置１と同一の暗号キーＱを作成する。またデスクランブル回路４７において、復調回路４４より出力される暗号化データをこの暗号キーＱによりデスクランブル処理し、元のメッセージＰ２を復号する。さらに制御部４５において、これらのメッセージに付加された位置データに基づいて、メッセージ部のデータを選択入力し、これにより照合結果、制御コマンドに応答するステータスデータを取得する。

【００２５】また外部機器７の制御部４５において、同様に制御コマンド、この制御コマンドに付随するデータでなる照合対象の画像データによりメッセージ部を形成し、このメッセージ部に冗長データ、位置データ、ランダムデータを付加してメッセージＰ１を形成する。さらにスクランブル回路４８において、このメッセージＰ１をスクランブル処理することにより、暗号化データＭ１（＝Ｅｎｃ（Ｑ、Ｐ１））を生成し、この暗号化データＭ１が変調回路４９により変調されて指紋照合装置１に入力される。

【００２６】指紋照合装置１において、復調回路５１は、この外部機器７より伝送された暗号化データを復号し、続くデスクランブル回路５２は、暗号キーＱによりこの暗号化データＭ１を処理し、これにより元のメッセージＰ１（＝Ｄｅｃ（Ｑ，Ｍ１））を復号する。なおここでＤｅｃ（Ｑ，Ｍ１）は、暗号キーＱにより暗号化データＭ１を復号する関数である。制御部３においては、このメッセージＰ１に付加された位置データを基準にして、メッセージ部を選択的に入力し、これにより外部機器７より送出された制御コマンド、照合対象の画像データを取得する。

【００２７】（１－２）暗号キーの更新

ところでこのようにして全ての入出力データを暗号化し、また同一のデータが伝送されないようにしても、継続した盗聴等により暗号キーＱが第３者に取得される場合も考えられることにより、この実施の形態では、外部機器７の制御により、一定周期で図４に示す処理手順を実行し、これにより暗号キーＱを更新する。

【００２８】すなわち制御部３は、外部機器７よりメッセージが到来すると、ステップＳＰ１よりステップＳＰ２に移り、このメッセージを解析し、キー更新コマンドが入力されたか否か判断する。ここで否定結果が得られると、制御部３は、ステップＳＰ３に移り、対応する処理手順を実行した後、ステップＳＰ４に移ってこの処理手順を終了する。

【００２９】これに対して受信した制御コマンドがキー更新コマンドの場合、制御部３は、ステップＳＰ２からステップＳＰ５に移り、パラメータＫの更新コマンドか否か判断する。ここでこの実施の形態において、外部機器７は、図１について上述した暗号キーＱの生成に必要なパラメータＫ又はＢを、キー更新の制御コマンドと共に、図３のフォーマットにより伝送する。

【００３０】制御部３は、このステップＳＰ５において、肯定結果が得られると、ステップＳＰ６に移り、パラメータＫを取得して暗号キー生成回路４１にセットし、続くステップＳＰ７においてこの暗号キー生成回路４１で生成される暗号キーＱを更新する。これに応動して外部機器７においては、同様の処理を実行し、この指紋照合装置１と同一の暗号キーＱをセットする。なお指紋照合装置１及び外部機器７においては、ディフォルトのパラメータＫ及びＢを有し、これにより例えば設置直後においては、このディフォルトのパラメータＫ及びＢにより通信して、このシステム固有の暗号キーを設定するようになされている。

【００３１】これに対してステップＳＰ５において、否定結果が得られると、この場合入力された制御コマンドがパラメータＢの更新コマンドでなることにより、制御部３は、ステップＳＰ８に移り、パラメータＢを取得して暗号キー生成回路４１にセットし、続くステップＳＰ７においてこの暗号キー生成回路４１で生成される暗号キーＱを更新する。これに応動して外部機器７においては、同様の処理を実行し、この指紋照合装置１と同一の暗号キーＱをセットする。

【００３２】（２）実施の形態の動作

以上の構成において、指紋照合装置１は（図１）、所定の操作子の操作により、指紋読み取り部４において照合対象でなる指紋の画像が取得され、画像照合部５のデータベースに登録された基準画像とこの指紋の画像とが照合され、入出力部６を介して照合結果が外部機器７に出力される。また同様に、外部機器７より入力される制御コマンドに応動して、指紋読み取り部４において照合対象でなる指紋の画像が取得され、画像照合部５のデータベースに登録された基準画像とこの指紋の画像とが照合され、入出力部６を介して照合結果が外部機器７に出力される。さらに外部機器７の制御コマンドに付加された画像データを照合対象の指紋画像に設定して、画像照合部５のデータベースに登録された基準画像とこの指紋の画像とが照合され、入出力部６を介して照合結果が外部機器７に出力される。

【００３３】またこれらの処理の他に、所定の操作子の操作により、指紋読み取り部４において取得された指紋の画像が画像照合部５のデータベースに基準画像として登録され、また同様に、外部機器７の制御コマンドに付加された画像データが画像照合部５のデータベースに登

録される。

【００３４】これらの処理において、指紋照合装置１においては、制御コマンドに応答するステータスデータ、照合結果のデータが外部機器７に送出され、また外部機器７からは、制御コマンド、制御コマンドに付随する画像データ等が指紋照合装置１に伝送される。

【００３５】これらのデータは（図３）、所定のパケット構造によるメッセージＰ１、Ｐ２に形成された後、指紋照合装置１及び外部機器７で共通の暗号キーＱにより各スクランブル回路４２、４８においてスクランブル処理され、暗号化されて伝送される。これにより指紋照合装置１では、セキュリティーが確保される。

【００３６】このようにしてパケット構造のメッセージＰ１、Ｐ２に形成される際に、これらのデータは、冗長なデータ、メッセージ部の位置を示す位置データ、ランダムなデータが付加されて一定のデータ量により形成され、これにより例えば同一の照合ＯＫのメッセージを送出する場合でも、伝送の都度異なる暗号化データにより伝送対象に送出される。これによっても、この指紋照合装置１では、システムの信頼性が図られる。

【００３７】このようにして暗号キーＱにより暗号化して種々のデータを送受するにつき、このシステムに設定された一定の周期により、暗号キーＱの更新処理が実行される（図４）。すなわち外部機器７より、暗号キーの生成に必要なパラメータＫ又はＢがメッセージ部に割り当てられて、それまでの暗号キーＱにより暗号化されて伝送される。さらにこのパラメータＫ又はＢにより、それぞれ指紋照合装置１及び外部機器７において、暗号キーＱが更新される。

【００３８】これにより暗号キーＱが解読された場合でも、新たな暗号キーＱにより種々のデータを送受することができ、信頼性を向上することができる。またこのとき暗号キーＱの生成に必要なパラメータのみ伝送し、暗号キー変換回路４１、４６による演算処理により暗号キーＱを生成することにより、直接暗号キーＱを伝送する場合に比して信頼性を向上することができる。

【００３９】（３）実施の形態の効果

以上の構成によれば、暗号キーの生成に必要なパラメータの伝送により暗号キーを更新することにより、照合結果を含む種々のデータを暗号化して伝送するにつき、伝送路を介して実行される不正行為を有効に回避することができ、これによりこの種のシステムのセキュリティーを向上することができる。

【００４０】またこのとき、ランダムなデータ、位置データを付加してスクランブル処理してパラメータを伝送することにより、このパラメータ自体の不正な取得をも低減することができ、その分さらに一段とセキュリティーを向上することができる。

【００４１】（４）他の実施の形態

なお上述の実施の形態においては、指紋読み取り手段で読み取る指紋画像だけでなく外部機器より入力される指紋画像を処理する場合について述べたが、本発明はこれに限らず、単に指紋読み取り手段で読み取る指紋画像を処理する場合にも広く適用することができる。

【００４２】また上述の実施の形態においては、いわゆるＳＡＬＴの手法を適用する場合について述べたが、本発明はこれに限らず、種々の手法により同一のデータを異なるデータにより伝送する場合に広く適用することができる。

【００４３】さらに上述の実施の形態においては、本発明を指紋照合装置に適用する場合について述べたが、本発明はこれに限らず、例えば印影の照合装置、網膜の照合装置等に広く適用することができる。

【００４４】また上述の実施の形態においては、本発明を指紋照合装置でなる画像照合装置に適用する場合について述べたが、本発明はこれに限らず、例えば音声認識による個人を識別して登録された個人か否か識別する音声照合装置等、入力手段を介して得られる個々のデータを基準データと比較して照合結果を出力する照合装置に広く適用することができる。

【００４５】

【発明の効果】上述のように本発明によれば、照合結果等を暗号化して伝送するにつき、パラメータの伝送により暗号キーを更新することにより、システムのセキュリティーを向上することができる。

【図面の簡単な説明】

【図１】本発明の実施の形態に係る指紋照合装置の入出力部を示すブロック図である。

【図２】図１の指紋照合装置を示すブロック図である。

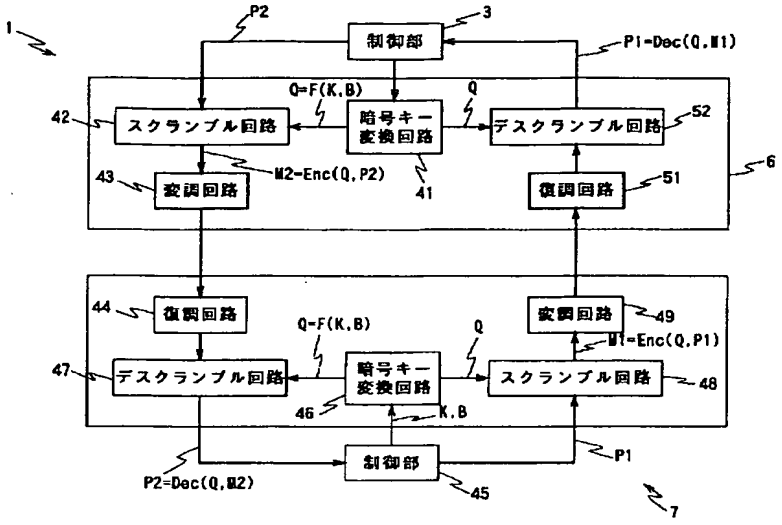
【図３】伝送に供するデータフォーマットの説明に供する略線図である。

【図４】暗号キーの更新処理の説明に供するフローチャートである。

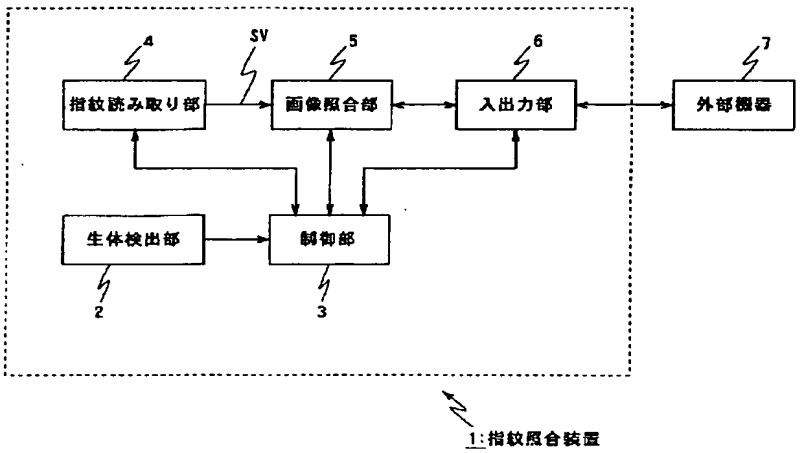
【符号の説明】

１……指紋照合装置、２……生体検出部、３……制御部、４……指紋読み取り部、５……画像照合部、６……入出力部、７……外部機器、４１、４６……暗号キー変換回路、４２、４８……スクランブル回路、４７、５２……デスクランブル回路

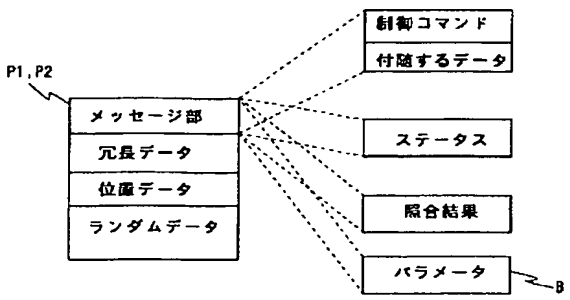
【図１】


1
P2
制御部
3
P1=Dec(Q,M1)
Q=F(K,B)
Q
42
スクランブル回路
暗号キー変換回路
デスクランブル回路
52
43
変調回路
M2=Enc(Q,P2)
41
復調回路
51
6
44
復調回路
Q=F(K,B)
Q
変調回路
49
M1=Enc(Q,P1)
47
デスクランブル回路
暗号キー変換回路
スクランブル回路
48
46
K,B
制御部
P1
P2=Dec(Q,M2)
45
7

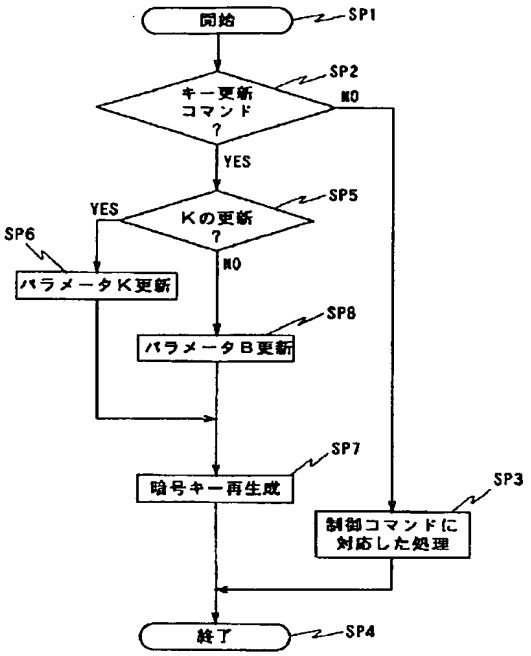
【図２】


4
SV
5
6
7
指紋読み取り部
画像照合部
入出力部
外部機器
生体検出部
制御部
2
3
1:指紋照合装置

【図３】


P1,P2
メッセージ部
冗長データ
位置データ
ランダムデータ
制御コマンド
付随するデータ
ステータス
照合結果
パラメータ
8

【図４】


開始
SP1
キー更新コマンド？
SP2
NO
YES
Kの更新？
SP5
YES
SP6
パラメータK更新
NO
パラメータB更新
SP8
暗号キー再生成
SP7
制御コマンドに対応した処理
SP3
終了
SP4